Kiteworks

TECHNISCHER LEITFADEN

MOVEit: Drei-Jahres-Bilanz der Schwach-stellen

Historischer Vorfallsbericht, Analyse der Sicherheits-architektur, regulatorische Implikationen und die architektonische Alternative

Im Mai 2023 wurde eine kritische SQL-Injection-Schwachstelle in Progress MOVEit Transfer (CVE-2023-34362) zum Vehikel für eine der größten je dokumentierten Lieferketten-Datenschutzverletzungen. Drei Jahre später hat MOVEit mindestens 11 offengelegte CVEs über drei Produktlinien hinweg angesammelt, darunter fünf mit einer NVD-CVSS-Bewertung von 9.0 oder höher, und die Plattform bleibt in aktiven Ausnutzungszyklen. Die Offenlegung vom 30. April 2026 von **CVE-2026-4670** (Authentifizierungs-Bypass mit CVSS 9.8) und **CVE-2026-5174** in MOVEit Automation markiert die dritte Welle kritischer Schwachstellen, die die Plattform in drei Jahren trifft.

Diese vertiefte Analyse untersucht, was die MOVEit-Bilanz den Sicherheits- und Compliance-Verantwortlichen über die Architektur von Managed File Transfer als Kategorie sagt. Das Muster ist strukturell -- eine Eigenschaft von Plattformen, die eine internetexponierte Oberfläche, kundenseitig verwaltete Infrastruktur, sensible Inhalte im Ruhezustand und begrenzte Eindämmung bei entdeckten Schwachstellen kombinieren. Die architektonische Antwort ist nicht ein anderes MFT-Produkt. Es ist ein völlig anderes Modell.

Was dieser Bericht aussagt

Das MOVEit-Schwachstellenmuster ist keine Pechsträhne. Es ist das vorhersehbare Ergebnis einer Architektur, die eine internetexponierte Webanwendung, ein kundenseitig verwaltetes Betriebssystem, ein SQL-Backend und einen Dateispeicher auf einer einzigen Vertrauensgrenze platziert.

Ein MFT-Anbieterwechsel setzt den Patch-Zyklus zurück. Ein Architekturwechsel beendet ihn.

11+ offengelegte MOVEit-CVEs über drei Produktlinien in drei Jahren

5 mit NVD CVSS 9.0 oder höher -- kritischer Schweregrad

1.440+ internetexponierte MOVEit-Automation-Instanzen heute gefährdet

1

Drei-Jahres-Bilanz

Auf einen Blick

2023

Cl0p nutzt MOVEit Transfer massenhaft aus. Über 2.700 Organisationen, ~93 Mio. Personen.

2024

Zwei Authentifizierungs-Bypässe mit NVD CVSS 9.1. Exploit-Code am ersten Tag öffentlich.

2025

Privilege Escalation im SFTP-Shared-Accounts-Modul.

2026

Authentifizierungs-Bypass mit NVD CVSS 9.8 + Privilege Escalation in MOVEit Automation. Kein Workaround.

Die Cl0p-Massenausnutzung von 2023 und die nachfolgenden CVEs

Am 27. Mai 2023 begann die Ransomware-Gruppe Cl0p mit der Massenausnutzung von CVE-2023-34362, einer SQL-Injection-Schwachstelle mit CVSS 9.8 in MOVEit Transfer. Progress veröffentlichte am 31. Mai einen Patch, doch in einigen Fällen beobachtete Mandiant Datendiebstahl **innerhalb von Minuten nach der Web-Shell-Entwicklung** -- der Patch kam nach dem größten Teil des Schadens. Die Angriffskette kombinierte SQL-Injection in der Webanwendung, eine Deserialisierungsschwachstelle, die das daraus resultierende Sysadmin-Token in Remote Code Execution umwandelte, und das Fehlen architektonischer Eindämmung zwischen der Anwendung und dem zugrunde liegenden Azure Blob Storage. Cl0p installierte eine angepasste ASP.NET-Web-Shell namens LEMURLOOT, getarnt als *human2.aspx*, die versteckte Administratorkonten mit der Bezeichnung „Health Check Service“ erstellte und Daten über angepasste HTTP-Header exfiltrierte.

Wie die Cl0p-Angriffskette von 2023 die Daten erreichte

1 SQL-Injection in der Web-Schicht

Unauthentifizierte SQL-Injection in der öffentlichen MOVEit-Transfer-Weboberfläche -- der für den Partnerzugriff erforderlichen Oberfläche -- legte Tokens mit Sysadmin-Berechtigung offen.

2 Deserialisierung zu Remote Code Execution

Eine Deserialisierungsschwachstelle wandelte das erbeutete Token in beliebige Codeausführung auf dem Host um. Webanwendung und Datenbank führten nun die Anweisungen des Angreifers aus.

3 LEMURLOOT-Web-Shell installiert

Eine angepasste ASP.NET-Web-Shell (human2.aspx) erstellte versteckte Administratorkonten namens „Health Check Service“ und leitete die Exfiltration über angepasste HTTP-Header.

4 Direkter Zugriff auf den Dateispeicher

Keine Schichtgrenze trennte die Anwendung vom Dateispeicher oder den Azure-Blob-Zugangsdaten. Einmal drinnen, deckte der Schadensradius jede Kundendatei ab, die die Plattform speicherte.

Bis Ende 2023 hatte die Kampagne über 2.700 Organisationen kompromittiert und personenbezogene Daten von etwa 93,3 Millionen Personen offengelegt. Die CISA schätzte, dass über 3.000 US-Einrichtungen und über 8.000 weltweit betroffen waren, wenn die nachgelagerte Exposition einbezogen wurde -- mehr als vier von fünf Opferorganisationen hatten keine direkte Beziehung zu Progress. In den sechs Wochen nach der ursprünglichen Offenlegung identifizierte Progress fünf weitere CVEs: CVE-2023-35036 (9. Juni), CVE-2023-35708 (15. Juni) und das Juli-Service-Pack, das CVE-2023-36932, CVE-2023-36933 und CVE-2023-36934 (CVSS 9.1 kritisch) behandelte.

Genannt in den Cl0p-Offenlegungen zu MOVEit Transfer im Jahr 2023

BBC	British Airways	US-Energieministerium	Johns Hopkins University
Shell	Louisiana Airways	Oregon DMV	Maximus (11,3 Mio.)
Welltok (10 Mio.)	Delta Dental of CA (6,9 Mio.)	CMS / WPS (3,1 Mio.)	+ 2.700 weitere

Das Authentifizierungs-Bypass-Paar von 2024

Am 25. Juni 2024 gab Progress **CVE-2024-5805** (kritischer Authentifizierungs-Bypass mit CVSS 9.1 in MOVEit Gateway) und **CVE-2024-5806** (anfangs CVSS 7.4, zwei Tage später auf 9.1 kritisch hochgestuft, als eine Schwachstelle der Drittanbieter-Bibliothek IPWorks SSH offengelegt wurde) bekannt. Beides waren Schwachstellen durch fehlerhafte Authentifizierung im SFTP-Modul. Die Shadowserver Foundation beobachtete innerhalb weniger Stunden nach der Offenlegung Ausnutzungsversuche gegen CVE-2024-5806. WatchTowr Labs veröffentlichte am selben Tag funktionsfähigen Proof-of-Concept-Exploit-Code. Die Ausnutzung erforderte lediglich einen gültigen Benutzernamen, erreichbar durch Credential Spraying gegen den SFTP-Dienst.

“Ausnutzungsversuche erfolgten innerhalb weniger Stunden nach der Offenlegung. Funktionsfähiger Proof-of-Concept-Code war am selben Tag öffentlich. Die Ausnutzung benötigte lediglich einen gültigen Benutzernamen.” -- Authentifizierungs-Bypass in MOVEit Gateway / Transfer -- Juni 2024

Das Privilege-Escalation-Problem von 2025 und die Offenlegung von 2026

Im Jahr 2025 gab Progress **CVE-2025-2324** bekannt, eine Schwachstelle durch fehlerhafte Privilegienverwaltung im SFTP-Modul von MOVEit Transfer, die als Shared Accounts konfigurierte Benutzer betraf. Die Mitteilung vom 30. April 2026 gab anschließend **CVE-2026-4670** und **CVE-2026-5174** in MOVEit Automation bekannt, der Produktlinie, die MFT-Vorgänge automatisiert und plant -- Lohnabrechnungen, Krankenversicherungsforderungen, Finanztransaktionen, behördliche Einreichungen. Shodan identifizierte über 1.440 internetexponierte MOVEit-Automation-Instanzen in Gefahr, darunter 16, die mit US-Landes- und Kommunalbehörden verbunden waren.

Das herstellerübergreifende Muster: vier kritische MFT-Schwachstellen in 18 Monaten

MOVEit ist das am häufigsten behandelte Beispiel, aber das Muster ist nicht auf einen Anbieter beschränkt. Im Verlauf von 2024 und 2025 veröffentlichten vier verschiedene MFT-Plattformen Schwachstellen mit kritischem Schweregrad, von denen jede innerhalb eines kurzen Zeitfensters nach der öffentlichen Offenlegung ausgenutzt wurde.

Cleo — Dez. 2024

Cl0p-Massenausnutzung; 300+ erklärte Opfer in Transport, Fertigung und Lebensmittel.

CrushFTP — März 2025

Authentifizierungs-Bypass; die nachfolgende Offenlegung im Juli 2025 ermöglichte die vollständige Serverübernahme.

Wing FTP — Juli 2025

Unauthentifizierte RCE durch Lua-Injection; Auswirkung auf root-/SYSTEM-Privilegien.

MOVEit — Apr. 2026

Authentifizierungs-Bypass mit NVD CVSS 9.8 + Privilege Escalation in Automation. Kein Workaround.

MOVEit-CVE-Historie, 2023-2026

Jahr	CVE	Vektor	CVSS NVD	Auswirkung
2023	CVE-2023-34362	SQL-Injection (Transfer)	9.8	Cl0p-Zero-Day; 2.700+ Orgs, 93 Mio.+ Personen
2023	CVE-2023-35036	SQL-Injection (Transfer)	Kritisch	Folgeoffenlegung am 9. Juni
2023	CVE-2023-35708	SQL-Injection (Transfer)	Kritisch	Folgeoffenlegung am 15. Juni
2023	CVE-2023-36932	SQL-Injection (Transfer)	Hoch	Juli-Service-Pack
2023	CVE-2023-36933	Unbehandelte Ausnahme	Hoch	Juli-Service-Pack
2023	CVE-2023-36934	SQL-Injection (Transfer)	9.1	Juli-Service-Pack
2024	CVE-2024-5805	Auth-Bypass (Gateway SFTP)	9.1	Offengelegt am 25. Juni; PoC am selben Tag
2024	CVE-2024-5806	Auth-Bypass (Transfer SFTP)	9.1	Shadowserver-Ausnutzung innerhalb von Stunden
2025	CVE-2025-2324	Privilege Escalation (SFTP)	Hoch	Shared-Accounts-Modul
2026	CVE-2026-4670	Auth-Bypass (Automation)	9.8	Aktueller Hinweis; kein Workaround
2026	CVE-2026-5174	Eingabevalidierung (Automation)	8.8	Verkettet mit CVE-2026-4670

2

Warum die Architektur weiter versagt

MOVEit ist ein für die Kategorie typisches Managed-File-Transfer-Produkt: eine Webanwendung, die auf kundenseitig verwalteter Windows-Infrastruktur läuft, gestützt durch eine SQL-Server-Datenbank, optional mit einer vorgeschalteten Gateway-Komponente und Dateien im Ruhezustand im lokalen Dateisystem oder im Azure Blob Storage. Vier architektonische Eigenschaften ergeben gemeinsam das CVE-Muster.

Die strukturelle Lesart

Jede der folgenden vier Eigenschaften ist für die MFT-Kategorie normal. In einer einzigen Vertrauensgrenze kombiniert, ergeben sie den Fehlermodus, den die CVE-Bilanz dokumentiert.

1. Internetexponierte Webanwendungsoberfläche

Die öffentliche Weboberfläche ist für den Partnerzugriff erforderlich. Jede offengelegte SQL-Injection, jeder Authentifizierungs-Bypass und jede Eingabevalidierungs-Schwachstelle erreicht die Plattform über diese Oberfläche.

2. Kundenseitig verwaltete Infrastruktur

Die Sicherheit hängt davon ab, dass der Kunde Windows, IIS, SQL Server und das Netzwerk korrekt härtet. Jede Fehlkonfiguration ist eine potenzielle CVE in der Betriebsumgebung.

3. Keine Eindämmung, sobald drinnen

Sobald ein Angreifer RCE erlangt hat, isoliert nichts die Anwendung von der Datenbank, dem Dateispeicher oder den Azure-Blob-Zugangsdaten. Der Schadensradius ist total.

4. Patch-Zyklus ohne Workaround

Jede offengelegte CVE erforderte ein Vollinstaller-Upgrade. In mehreren Fällen wurde Ausnutzung innerhalb weniger Stunden nach der Offenlegung beobachtet. Der Zyklus summiert sich.

3

Regulatorische Implikationen

MFT-Plattformen sitzen am Datenaustausch-Engpass für regulierte Workloads: geschützte Gesundheitsdaten unter HIPAA, kontrollierte nicht-klassifizierte Informationen unter CMMC und DFARS, Karteninhaberdaten unter PCI DSS, personenbezogene Daten unter DSGVO und einzelstaatlichen Datenschutzgesetzen, Finanzunterlagen unter SOX und SEC-Vorschriften. Wenn die MFT-Plattform das Vehikel der Datenschutzverletzung ist, trägt der Kunde die regulatorische Exposition -- nicht Progress. Jede MOVEit-Offenlegung verkürzt zudem die verfügbare regulatorische Verteidigung: Die Cl0p-Kampagne von 2023 war ein Zero-Day, das Authentifizierungs-Bypass-Paar von 2024 wurde mit funktionsfähigem Exploit-Code am ersten Tag offengelegt, und bei der Offenlegung von 2026 sind über 1.440 internetexponierte Instanzen gefährdet.

Regime	Norm	Exposition	MOVEit-bezogener Auslöser
USA Bund	SEC Item 1.05 (Dez. 2023)	Öffentliche 8-K-Offenlegung eines wesentlichen Vorfalls in 4 Werktagen	Die SEC eröffnete am 2. Oktober 2023 eine formelle Untersuchung von Progress
USA Gesundheit	HIPAA Security Rule 45 CFR §164.308	OCR-Standard für angemessene Sicherheitsmaßnahmen; Zivilstrafen bis zu 2,1 Mio. USD pro Jahresobergrenze je Verstoßstufe	CMS/WPS-Verletzung an OCR gemeldet, betraf 3,1 Mio. Personen
USA Verteidigung	CMMC Level 2 / DFARS 252.204-7012	C3PAO-Bewertung erforderlich; DoD-Vorfallsmeldung innerhalb von 72 Stunden	Internetexponierte MFT betrifft direkt SC.L2-3.13.1, SC.L2-3.13.5, AC.L2-3.1.20
EU	Artikel 32 DSGVO + NIS 2 (Okt. 2024)	Bis zu 4 % des globalen Umsatzes; Frühwarnung in 24 Std. / Vorfallsmeldung in 72 Std.	Die ICO verhängte im Okt. 2025 eine Strafe von 14 Mio. £ gegen Capita unter Berufung auf Artikel 32
Australien	APP 11 + Privacy Amendment Act 2024	Bis zu 50 Mio. AUD oder 30 % des bereinigten Umsatzes bei schweren oder wiederholten Verstößen	OAIC-NDB-Meldungen +25 % gegenüber dem Vorjahr in 2024; das Medibank-Verfahren schafft Präzedenz

„Die Frage der Aufsichtsbehörde ist nicht, ob die Datenschutzverletzung vorhersehbar war. Sie lautet, ob der Weiterbetrieb der Plattform nach drei Wellen kritischer Schwachstellen in drei Jahren eine angemessene Schutzmaßnahme darstellt.“

4

Die architektonische Alternative

MOVEit gegen ein anderes MFT-Produkt zu tauschen, setzt die Patch-Zyklus-Uhr zurück, ohne das zugrunde liegende Modell zu ändern. Die architektonische Antwort ist eine Plattform, die die Datenaustauschoberfläche auf einer gehärteten, mandantenisolierten virtuellen Appliance konsolidiert -- mit einer einzigen Richtlinien-Engine, einem einzigen Audit-Log und Sicherheit als Produktmerkmal statt als kundenseitige Konfigurationslast.

Gehärtete virtuelle Appliance, keine kundenseitig verwaltete Infrastruktur

Kiteworks wird als gehärtete virtuelle Appliance mit eingebetteter Netzwerk-Firewall, eingebetteter Web Application Firewall, eingebetteter Intrusion Detection und einem reduzierten, von Kiteworks gepflegten Betriebssystem bereitgestellt. Kunden konfigurieren das Betriebssystem nicht, verwalten die Datenbank nicht und patchen den zugrunde liegenden Stack nicht separat. Vollsystem-Updates per Mausklick patchen die gesamte Appliance -- Anwendung, Runtime, Betriebssystem, Bibliotheken -- in einem einzigen koordinierten Vorgang.

Verteidigung in der Tiefe, nachgewiesen

Während des Log4Shell-Vorfalls im Dezember 2021 lag der branchenweite NVD-CVSS-Wert für die zugrunde liegende Log4j-Schwachstelle bei 10,0.

Die mehrschichtigen Kontrollen von Kiteworks dämmten die praktische Ausnutzbarkeit von Log4Shell in unserer Umgebung ein, bevor der formelle Patch eintraf. Die interne Bewertung von Kiteworks schätzte die verbleibende Ausnutzbarkeit auf etwa CVSS 4,0; diese Zahl ist eine interne Schätzung, keine offiziell vom NIST oder der CVE Numbering Authority vergebene CVSS-Bewertung.

Verteidigung in der Tiefe ist hier nicht theoretisch -- sie ist der Grund, warum ein NVD CVSS von 10 eingedämmt blieb.

Mandantenisolierung und FIPS-140-3-Verschlüsselung

Jede Kiteworks-Bereitstellung ist mandantenisoliert konzipiert -- keine gemeinsam genutzten Datenbanken, Dateisysteme oder Laufzeiten zwischen Kunden. Intern isoliert eine mehrstufige Architektur die Web-Schicht von der Datenbank und dem Dateispeicher, sodass eine kompromittierte Anwendungsschicht weder die Datenbank direkt abfragen noch Schlüssel auf Dateiebene ableiten kann. Dateien im Ruhezustand sind durch zwei unabhängige Verschlüsselungsschichten geschützt (auf Datei- und Festplattenebene) mittels FIPS-140-3-validierter Kryptomodule, mit TLS 1.3 in Übertragung und optionalem kundenseitig kontrolliertem Schlüsselmanagement für Souveränitäts-Workloads.

MOVEit-Architektur vs. Kiteworks-Architektur

Sechs architektonische Eigenschaften unterscheiden die beiden Plattformen. Jede entspricht direkt einem der in der MOVEit-Bilanz dokumentierten Fehlermodi. Offenlegungsdatum des Vergleichs: 12. Mai 2026. Die Charakterisierung von MOVEit spiegelt die Plattform wider, wie sie von Progress zum Zeitpunkt der Mitteilung vom 30. April 2026 dokumentiert wurde; Produktfunktionen und Bereitstellungsoptionen können sich in späteren Progress-Versionen ändern.

Dimension	MOVEit-Architektur	Kiteworks-Architektur
Infrastruktur	Vom Kunden verwaltete Windows Server, IIS und SQL Server; vom Kunden gehärtetes Betriebssystem und Netzwerk	Von Kiteworks gepflegte gehärtete virtuelle Appliance; eingebettete Firewall, WAF und IDS; Updates per Mausklick
Eindämmung	Die Webanwendung hat direkten Zugriff auf alle Kundendateien und die Datenbank	Mehrstufige Architektur; die Web-Schicht kann weder auf den Dateispeicher zugreifen noch Schlüssel auf Dateiebene ableiten
Datenschutz	Verschlüsselung auf Anwendungsebene; Anwendungs-Logs; SIEM-Integration liegt in der Verantwortung des Kunden	FIPS-140-3-Doppelschicht-Verschlüsselung (Datei + Festplatte); manipulationssicheres Audit-Log; SIEM-Lieferung in Echtzeit
Privilegierter Administratorzugriff	Die Administratorkonsole ist das Windows-Betriebssystem selbst, sodass Administratoren auf Servercode und Dateisystem zugreifen und Anwendungen installieren können. Angreifer, die privilegierten Zugriff auf die Konsole erlangen, können eigenen Code für Aufgaben wie Fernsteuerung und Datenexfiltration installieren.	Administratoren haben keinen Zugriff auf das Betriebssystem, das Dateisystem, den Anwendungscode oder die Datenbank, die sich vollständig innerhalb der gehärteten virtuellen Appliance befinden. Die Administratorkonsole ist eine Weboberfläche mit strengen rollenbasierten Zugriffskontrollen (System, Anwendung, Support, benutzerdefiniert); Administrationsfunktionen verändern das System ausschließlich über bestimmte API-Aufrufe, und Administratoren können keine Software auf der Appliance installieren.
Benutzerverwaltung	Verwendet die Windows-Benutzerverwaltung als Anwendungsbenutzerverwaltung. Je nach Konfiguration kann der Schadensradius über die MOVEit-Umgebung hinausreichen.	Speziell entwickeltes Benutzerverwaltungssystem, vollständig getrennt von der Benutzerverwaltung des Betriebssystems
Patch-Kadenz	Drei kritische Wellen in drei Jahren; keine Workarounds; Notfall-Änderungsfenster	Routinemäßiges Anbieter-Patch-Ereignis; die praktische Ausnutzbarkeit von Log4Shell wurde durch mehrschichtige Kontrollen vor Eintreffen des Patches eingedämmt

Wenn Sie heute MOVEit Automation betreiben

Vier Maßnahmen, die sich diese Woche lohnen

- Patchen Sie auf MOVEit Automation 2025.1.5, 2025.0.9 oder 2024.1.8 mit dem Vollinstaller -- Progress bestätigt, dass es für CVE-2026-4670 und CVE-2026-5174 keinen Workaround gibt.
- Inventarisieren Sie internetexponierte Automation-Instanzen und prüfen Sie Audit-Logs auf Kompromittierungsindikatoren in den Command-Port-Schnittstellen des Service-Backends.
- Setzen Sie eine architektonische Überprüfung auf den nächsten Planungszyklus. Die Frage ist nicht mehr, ob gepatcht wird -- sondern, ob das Plattformmodell nach drei kritischen Wellen in drei Jahren weiterhin vertretbar ist.
- Sprechen Sie mit Kiteworks über eine architektonische Überprüfung in 30 Minuten -- sehen Sie, wie ein gehärtetes, mandantenisoliertes Appliance-Modell den Schadensradius beim nächsten MFT-Klasse-CVE verändern würde.

Rechtlicher Hinweis

Diese Analyse basiert auf öffentlich offengelegten Sicherheitshinweisen, Drittanbieter-Recherchen und der architektonischen Bewertung von Kiteworks zum 11. Mai 2026. Die technischen Eigenschaften von Drittanbieterprodukten können sich ändern. Dieses Dokument stellt keine Rechts- oder Sicherheitsberatung dar.

Kiteworks

Mai 2026